Amendments to the Claims:

This listing of claims replaces all prior listings, and versions, of claims in the present application.

Listing of Claims:

1-3. (Canceled)

4. (Currently Amended) The method of Claim 9 [[1]], wherein computing ~~selecting~~ the ~~a~~ first secret key further comprises selecting one of several predefined secret keys.

5. (Canceled)

6. (Currently Amended) The method of Claim 9 [[1]] further comprising obtaining the predefined key change information from a MAC data packet.

7. (Currently Amended) The method of Claim 9 [[1]], wherein combining the intermediate value with the predefined key change information further comprises performing a bitwise XOR operation.

8. (Currently Amended) A method for generating a temporary key for data encryption in a communication network, the method comprising the steps of:

generating an Initialization Vector (IV) value;

combining a first secret key with the IV value by performing a bitwise exclusive OR (XOR) operation to result in an intermediate value; and

permutating the intermediate value by exchanging a selected number of bits of the IV value with an equal number of other bits of the IV value and outputting a result of the [[a]]bitwise XOR operation and the exchange of the bits as a value that is bit shifted.

9. (Previously Presented) The method of Claim 8, further comprising computing the first secret key by selecting a predefined secret key, combining the predefined secret key with a user-specific Medium Access Control (MAC) address to result in the intermediate value, combining the intermediate value with predefined key change information and transforming the combination of the intermediate value and the predefined key change information by hashing to result in the first secret key.

10. (Original) The method of Claim 8, wherein generating an Initialization Vector (IV) value further comprises the steps of:

concatenating a timer value and at least a portion of a MAC address to result in a seed value; and

applying the seed value to a random number generator to result in the IV value.

11. (Canceled)

12. (Currently Amended) A method for generating a key for data encryption in a communication network, the method comprising the steps of:

calculating a first secret key utilizing predefined key change information;

determining if the key change information has repeated; and

differently processing the first secret key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated,

wherein differently processing the first secret key comprises performing a bitwise shift of the first secret key in instances in which the key change information has repeated.

13. (Canceled)

14. (Previously Presented) The method of Claim 12 wherein calculating a first secret key further comprises the steps of selecting a predefined secret key, combining the predefined secret key with a user-specific Medium Access Control (MAC) address to result in a first intermediate value, combining the first intermediate value with predefined key change information, transforming the combination of the intermediate value and the predefined key change information by hashing to result in a temporary key, combining the temporary key and an IV value and permutating the combination of the temporary key and the IV value to result in the first secret key.

15. (Currently Amended) A method for generating a key for data encryption in a communication network, the method comprising the steps of:

selecting a first secret key;

generating a first temporary key based upon a combination of the first secret key with at least a portion of a user-specific Medium Access Control (MAC) address and further based upon predefined key change information and hashing;

generating a second temporary key based upon a combination of the first temporary key and an Initialization Vector (IV) value;

determining if the predefined key change information has repeated; and

generating the key for data encryption based upon the second temporary key and the determination if the predefined key change information has repeated,

wherein generating the key for data encryption comprises differently processing the second temporary key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated.

16. (Canceled)

17. (Currently Amended) A method according to Claim 15[[16]] wherein differently processing the second temporary key comprises performing a bitwise shift of the second temporary key in instances in which the key change information has repeated.

18. (Previously Presented) The method of Claim 15, wherein generating the first temporary key further comprises combining an intermediate value generated by the combination of the first secret key with at least a portion of the user-specific MAC address with the predefined key change information and thereafter transforming the combination of the intermediate value and the predefined key change information by hashing to generate the first temporary key.

19. (Original) The method of Claim 18 wherein transforming comprises hashing the combination of the intermediate value and the predefined key change information to generate the first temporary key.

20. (Previously Presented) The method of Claim 15, wherein generating the second temporary key comprises permutating the combination of the first temporary key and the IV value.

21. (Original) The method of Claim 15, wherein generating the second temporary key comprises generating the IV value by concatenating a timer value and at least a portion of a MAC address to result in a seed value and applying the seed value to a random number generator to result in the IV value.

22. (Currently Amended) A method for data encryption in a communication network, the method comprising the steps of:

generating a first temporary key based upon a combination of a first secret key with at least a portion of a user-specific Medium Access Control (MAC) address and further based upon predefined key change information and hashing;

generating a second temporary key based upon a combination of the first temporary key and an Initialization Vector (IV) value;

determining if the predefined key change information has repeated;

generating a final key based upon the second temporary key and the determination if the predefined key change information has repeated; ~~and~~

encrypting data transmitted via the communication network with the final key;

determining if the data is originally encrypted in accordance with a predetermined encryption technique; and

decrypting the data if the data is originally encrypted in accordance with the predetermined encryption technique, prior to encrypting the data transmitted via the communication network with the final key.

23. (Canceled)

24. (Currently Amended) A method according to Claim 22[[23]] wherein determining if the data is originally encrypted comprises determining if the data is originally encrypted in accordance with a WEP technique.

25. (Currently Amended) A computer program product readable by a machine and tangibly embodying a program of instructions executable by the machine to perform steps for data encryption, the program of instructions comprising the steps of:

generating a first temporary key based upon a combination of a first secret key with at least a portion of a user-specific Medium Access Control (MAC) address and further based upon predefined key change information and hashing;

generating a second temporary key based upon a combination of the first temporary key and an Initialization Vector (IV) value;

determining if the predefined key change information has repeated;

generating a final key based upon the second temporary key and the determination if the predefined key change information has repeated, wherein generating the key for data encryption comprises differently processing the second temporary key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated; and

encrypting data transmitted via the communication network with the final key.

26. (Original) The computer program product of Claim 25 wherein the program of instructions further comprises the steps of:

determining if the data is originally encrypted in accordance with a predetermined encryption technique; and

decrypting the data if the data is originally encrypted in accordance with the predetermined encryption technique, prior to encrypting the data transmitted via the communication network with the final key.

27. (Canceled)

28. (Previously Presented) The computer program product of Claim 25 wherein the step of differently processing the second temporary key comprises performing a bitwise shift of the second temporary key in instances in which the key change information has repeated.

29. (Original) The computer program product of Claim 25 wherein the step of generating the first temporary key further comprises combining an intermediate value generated by the combination of the first secret key with at least a portion of the user-specific MAC address with the predefined key change information and thereafter transforming the combination of the intermediate value and the predefined key change information to generate the first temporary key.

30. (Original) The computer program product of Claim 29 wherein transforming comprises hashing the combination of the intermediate value and the predefined key change information to generate the first temporary key.

31. (Previously Presented) The computer program product of Claim 25, wherein the step of generating the second temporary key comprises permutating the combination of the first temporary key and the IV value.

32. (Original) The computer program product of Claim 25, wherein the step of generating the second temporary key comprises generating the IV value by concatenating a timer value and at least a portion of a MAC address to result in a seed value and applying the seed value to a random number generator to result in the IV value.